



# UNITED STATES PATENT AND TRADEMARK OFFICE

AN  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/829,763	04/10/2001	Osamu Shibata	29288.0400	9593
20322	7590	04/07/2006	EXAMINER	
SNELL & WILMER ONE ARIZONA CENTER 400 EAST VAN BUREN PHOENIX, AZ 850040001				PICH, PONNOREAY
ART UNIT		PAPER NUMBER		
				2135

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/829,763	SHIBATA ET AL.
	Examiner Ponnoreay Pich	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 06 January 2006.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-9 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | Paper No(s)/Mail Date _____   |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|  | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

Claims 1-9 are pending. As agreed upon in the interview on 12/14/2005 with applicant's representatives, the examiner withdraws the prior art rejections indicated in the previous office action. However, please note new rejections below.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-5 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claims 1-5 recite a decryption device comprising various sections that are "operable to" perform certain recited functions. It is unclear whether those sections are actually performing the indicated actions or if the language used in the claims merely indicates an intended use for the sections. Using one of the limitations of claim 1 as an example, claim 1 recites "an internal-key storage section operable to store an internal-key". The examiner notes that if there is a reference which discloses an internal-key storage section, absent any prohibition which prevents it from storing an internal-key, the internal-key storage section is operable to store a key. The same can be said of the other sections recited in claims 1-5. Absent any prohibition in a reference keeping the sections from performing the intended use, the sections should be operable to perform the recited use.

2. As per claim 2, the claim is directed towards a decryption device according to claim 1. However, the operation section is recited as further including encryption sections. It is unclear if applicant is claiming a decryption device or a device which does encryption and decryption.
3. Claim 7 is dependent on claim 6. Claim 6 is a method for decrypting encrypted content, yet the steps recited in claim 7 is directed towards encrypting. It is unclear how the encrypting steps recited in claim 7 accomplish decrypting of encrypted content, especially since the last step of claim 7 results in encrypted content.

#### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al (US 5,923,754) in view of Venkatesan et al (US 6,801,999), herein Ven, and further in view of Sims (US 2002/0016919).

#### **Claims 1 and 6:**

As per claim 1, Angelo discloses the limitations of:

1. An internal-key storage section operable to store an internal key (Fig 2, items 42 and 44; col 3, lines 50-58; and col 4, lines 31-33).
2. A content-key storage section operable to store content-keys (Fig 3, items 62 and 64; col 3, lines 50-58; and col 4, lines 41-67).
3. An operation section, the operating section including:
  - a. A first decrypting section operable to, when an encrypted content-key is input to the operation section, decrypt the encrypted content-key using the internal-key so as to obtain a content-key and store the content-key in the content-key storage section (Fig 3, item 66; col 3, lines 58-62; and col 4, lines 59-61).
  - b. A second decrypting section operable to, when an encrypted content is input to the operation section, decrypt the encrypted content using the current value of the content-key storage section as a content-key so as to obtain a first output data and output the first output data to the outside of the decryption device (Fig 3, items 68-72; col 3, lines 58-62; and col 4, lines 61-67).

Angelo does not disclose a determination section operable to determine whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different. Angelo does not disclose the decryption of the encrypted content also being dependent on the determination section determining that the value of the content-key storage section in its initial state and the current value

of the content-key storage section are different. However, the examiner notes that applicant's specification does not define what is the "initial state". The examiner submits that in the broadest, reasonable sense, any state of the content-key storage section can be considered the "initial state" as compared to a later point in time. The examiner assumes the state of the storage section that is most recent in time is the "current state".

Further, Ven discloses using keys which expires after a given interval of time (col 7, lines 49-52). Ven discloses a client PC, i.e. decryption device, being unable to access protected objects/content until a new valid key was obtained (col 8, lines 37-56). One of ordinary skill should appreciate that when a new key has been obtained, the state of the key storage section would change from what it was before, i.e. the initial state. Sims discloses checking for keys which have been revoked/expired or banned (p10, paragraphs 108-109). At the time applicant's invention was made, it would have been obvious to one of ordinary skill to incorporate Ven and Sims's teaching with Angelo's invention according to the limitations recited in claim 1. One of ordinary skill would have been motivated to incorporate Ven's teachings because it would allow Angelo's invention to be more secure against piracy by protecting against "break-once-run-everywhere" (BORE) attacks (Ven: col 5, lines 16-21). One of ordinary skill would be motivated to incorporate Sims's teachings as it would allow the combination invention of Angelo and Ven to determine when someone is attempting to use an expired or banned key to decrypt media content. Note that in Ven's invention, there needs to be a way to determine if a key being used has expired or not; Sims's teachings

provides for the solution to this need. Note that as per Sims's teachings, if a decryption device was still using a key that had expired or been banned, then the content-key storage section's state had not changed from its initial state. One of ordinary skill should appreciate that decryption of encrypted content is dependent on having updated and valid keys, so decryption would fail.

Claim 6 is substantially similar to claim 1 except it is directed towards a method for decrypting encrypted content, the method being performed by the device of claim 1. It is rejected for substantially the same reasons given for claim 1.

**Claims 2 and 7:**

As per claim 2, Angelo further discloses:

1. A content-key generation section operable to generate a content-key used for encrypting a content based on random numbers and store the generated content-key in the content-key storage section (col 4, lines 41-52), wherein the operation section further includes:
2. A first encrypting section operable to encrypt the content-key used for encrypting a content so as to obtain an encrypted content-key and output the encrypted content-key outside of the decryption device (col 3, lines 51-62 and col 4, lines 57-59).
3. A second encrypting section operable to, when a content is input to the operation section, encrypt the content using the current value of the content-key storage section as a content-key so as to obtain a second output data and output the second output data to outside of the decryption device (col 3, lines 51-62).

Angelo does not explicitly disclose the encryption of the content being dependent on the determination section determining that the value of the content-key storage section in its initial state and the current value of the content-key storage section being different. However, the limitation is obvious to Angelo's modified invention. Note in Angelo's modified invention, as per Ven and Sims's teachings, expired keys would not be used—Ven discloses that as per his teachings, content will not be processed by the decryption device if the being used key has expired (col 8, lines 46-56).

Claim 7 is substantially similar to claim 2 except it is directed towards a method which utilizes the decryption device of claim 2 to perform the intended use of the device of claim 2. It is rejected for substantially the same reasons given for claim 2.

**Claim 3:**

As per claim 3, Angelo further discloses:

1. A mutual authentication section operable to determine whether or not a mutual authentication has been made between the mutual authentication section and a storage device which is located outside the decryption device, the encrypted content-key being stored in the storage device (col 4, lines 42-52).
2. Wherein the second decrypting section is operable to decrypt the encrypted content when the mutual authentication section determines that the mutual authentication has been made (col 4, lines 57-67).

**Claims 4 and 8:**

As per claim 4, Angelo further discloses:

1. The internal-key storage section is operable to store a plurality of internal-keys (col 4, lines 31-33 and Fig 2).
2. The internal-key storage section is operable to select one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption section (Fig 3). *Note that Sims also discloses this limitation (p9, paragraph 97).*

Claim 8 is substantially similar to claim 4 except it is directed towards a method which utilizes the decryption device of claim 4 to perform the intended use of the device of claim 4. It is rejected for substantially the same reasons given for claim 4.

**Claims 5 and 9:**

Angelo, Ven, and Sims disclose all the limitations of claim 1. Ven further discloses the second decrypting section is further operable to prevent decryption of the encrypted content (col 7, lines 48-51 and col 8, lines 46-51). Ven does not explicitly disclose the decryption is dependent on the determination section determining that the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same. However, as stated previously, applicant's specification does not define what is the "initial state". The examiner interprets any state of the content-key storage section as the initial state as compared to a later state in time. One of ordinary skill should appreciate that Ven keeping the decryption device from processing content if the value in the key storage section is the same (col 8, lines 46-51), i.e. if the key storage section has not yet obtain a key that has not expired,

reads on the above limitation. The technique of how Ven can make this determination is further disclosed by Sims (p10, paragraph 108). One of ordinary skill would have been motivated to incorporate Ven and Sims's teaching within Angelo's invention for the same reasons given in claim 1.

Claim 9 is substantially similar to claim 5 except it is directed towards a method which utilizes the decryption device of claim 5 to perform the intended use of the device of claim 5. It is rejected for substantially the same reasons given for claim 5.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

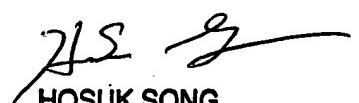
Ponnoreay Pich

Application/Control Number: 09/829,763  
Art Unit: 2135

Page 10

Examiner  
Art Unit 2135

PP

  
**HOSUK SONG**  
**PRIMARY EXAMINER**